Understanding Control Function and Failure From a Process Perspective

Heussen, Kai; Lind, Morten

Published in:
2012 IEEE Workshop on Complexity in Engineering

Link to article, DOI:
10.1109/CompEng.2012.6242946

Publication date:
2012

Understanding Control Function and Failure From a Process Perspective

Kai Heussen, Morten Lind
Department of Electrical Engineering
Technical University of Denmark
Kgs. Lyngby, Denmark
Email: kh@elektro.dtu.dk

***Abstract*—In control design, fault-identification and fault tolerant control, the controlled process is usually perceived as a dynamical process, captured in a mathematical model. The design of a control system for a complex process, however, begins typically long before these mathematical models become relevant and available. To consider the role of control functions in process design, a good qualitative understanding of the process as well as of control functions is required. As the purpose of a control function is closely tied to the process functions, its failure has a direct effects on the process behaviour and its function. This paper presents a formal methodology for the qualitative representation of control functions in relation to their process context. Different types of relevant process and control abstractions are introduced and their application to formal analysis of control failure modes from a process perspective is presented. Finally anticipated applications in context of offline analysis and online supervisory control are discussed.**

I. Introduction

In industrial practice, the high-level conception of control systems for complex plants has been an issue for some time [1]: "The central issue to be resolved by the new theories is the determination of the control system structure." The recent development of control applications for smart electricity systems and the needs are merely one additional application where the need for systematic approaches to support automation design at early stages can be emphasized [2].

In control engineering, however, there have been relatively few efforts in research on systematic approaches and formal representations of process and control functions that could support control structure design. In a series of article on plantwide control structure design for chemical engineering, Skogestad *et al.* [3], [4] review past efforts and outline a new systematic approach. The authors point out that in particular the concepts of abstraction and process decomposition suggested in past research on the subject lacks clarity and first principles: little is provided to guide the user with regard to why, when and where decompositions are required. Further they show that also unnecessary decompositions have been proposed, which reduce the performance of a control configuration. Their systematic approach is composed of a top-down analysis phase combined with a bottom-up design phase. One central tool for the top-down analysis is the degree-of-freedom (DOF) analysis. In the examples provided, this DOF analysis is based on a piping- and instrumentation diagram (PID) as process representation, which emphasizes the qualitative analysis aspect at this stage where the identification of inputs, outputs and control objectives is performed (loop pairing).

In control-engineering disciplines, mathematical approaches are often preferred to qualitative approaches, but the control-typical block-diagrams cannot be employed for the purpose as they require pre-selection of inputs and outputs (i.e. pre-assignment of causality). Mathematical modeling approaches that facilitate causality assignment are equation-based or behavioural modeling approaches, including bond-graph based methods [5]. When connected e.g. to an object-oriented modeling framework (such as e.g. MODELICA [6]), they offer a type of domain-representation that adds flexibility and simulation capabilites to the control design, supporting the protoptying of controllers and evaluation of alternatives. However, they also require a level of detail that often is simply not available in an earlier conceptual design phase – where control structure alternatives are developed and should be communicated.

Further, consider that a control objective, the anchoring purpose of a control function, is usually specified in terms of local process requirements rather than a central objective. Then a meaningful decomposition of a central objective cannot be derived from a mathematical process representation, but requires a functional understanding of the process design. Starting too early on mathematical representations thus limits the conception of meaningful abstraction levels from a process perspective.

A clear conceptual understanding of a process is also important during system operation. Consider that a plant operator (e..g of a power plant) needs to have a clear perspective on overall operating goals, while also fully grasping functions and behaviour of the process under control [7]. Also for the design of higher-level control aproaches, this need has been recognized. In a review on fault-tolerant control, Patton [8] writes: "[...] fault tolerant control should ideally be accompanied by a systematic and integrated approach to design", and continues, "[t]he strategy should [...] commence with an understanding of the structure of the system, the reliability of different components, the types of redundancy available [...] and the types of controller function which are available and might be required." The common representations avaialable and employed in control engineering do not satisfy these requirements.

In this paper it is discussed how a (qualitative!) functional

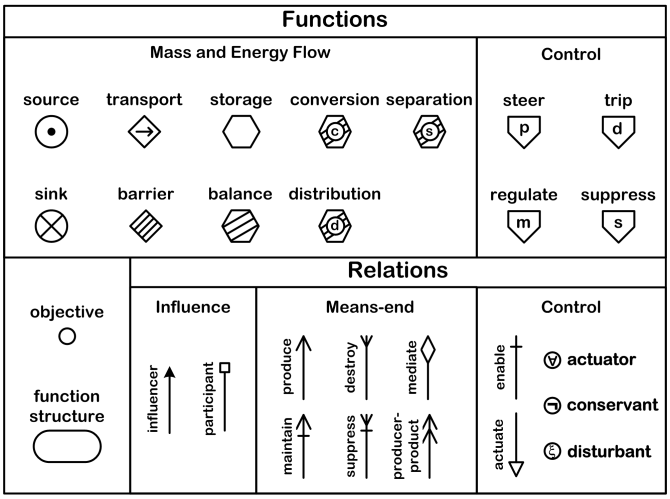

Fig. 1. MFM Concepts.

modeling approach called Multilevel Flow Modeling (MFM), adapted with recent extensions, can support the needs for process representation, relevant abstraction concepts as well as DOF analysis in early control structure design as well as in support of online operation. In the following section, the approach is briefly introduced. Then a result conveying an important abstraction concept and its realization on MFM models is presented. Finally, its application to control structure design and online operation and diagnosis is reflected upon.

II. Method

Multilevel Flow Modeling (MFM) is an approach to modeling goals and functions of complex industrial processes involving interactions between flows of mass, energy and information [9]. MFM has been developed to support functional modeling [10] of complex dynamic processes and combines means-end analysis with whole-part decompositions to describe the functions of the process under study and to enable modeling at different levels of abstraction.

MFM has been used to represent a variety of complex dynamic processes including fossil and nuclear power generation [11], several kinds of chemical processes (e.g. [12]), as well as electric power systems [2].

Applications of MFM include model based situation assessment and decision support for control room operators, hazop analysis [13], alarm design, alarm filtering [14] and planning of control actions [15], [16], [17]. MFM is supported by knowledge based tools for model building and reasoning [18].

A. MFM Concepts

MFM provides a diagrammatic notation of its elementary modeling concepts, as listed in Figure 1 and outlined below, together with syntactical and semantic rules for their interconnection. These basic concepts are developed along with a rigourous theoretical framework which shall be also be sketched below.

Process functions are represented by elementary *flow functions* interconnected to form *flow structures* with a common -conserved- flow object (*energy* or *mass*). Connections between functions within flow structures can be assigned with influencer roles (box or arrow-tip), indicating the assignment of active or passive participation in the transport of the flow object. Each flow structure represents a particular *goal*-oriented view of the system. *Objectives* can be combined with elementary *control functions* to form *control structures* [19]. Flow structures are interconnected in a multi-level representation through *means-end relations*, and *control relations*. Further, roles to model control influence on process functions have been introduced: actuator, conservant and disturbant [20].

The views represented by the flow structures, functions, objectives and their interrelations comprise a comprehensive model of the functional organization of the system represented as a hypergraph. MFM enables a formalized conceptual modeling of a system which support several forms of qualitative reasoning about control situations.

B. Underlying Concepts: Actions and Abstractions

The basic insight underlying MFM is that the functions of a complex process are composed of several levels of means and ends and that it takes a group of system functions to form a whole.

MFM functions are founded on fundamental concepts of action [21] and each of the elementary flow- and control functions can be seen as instances of more generic action types. The *action concept* further implies a pattern, defining for each function a) the action (action verb) represented and b) a number of required and optional (action-)*roles* such as agent, participant, object, etc.

All modeling in MFM is founded on a *means-ends* perspective: process levels are defined in terms of means and ends, and specific types of means-ends relations establish the relationship between process functions and objectives, as well as explicit dependency structures between process functions at different abstraction levels.

Function structures express the *whole-part* relation which identifies a set of functions that by their interactions form a purpose-oriented view of the system. The whole-part relations for flow-functions as well as reasoning about influence propagation are enabled by the conservation laws of mass and energy, which imply a rigorous mapping of states and constraints to functions. Here sources and sinks correspond to system boundaries. Each flow-function corresponds to a specific type of constraint with associated state variables.

In combination with the action concept this allows a mapping of semantic roles to the functional constraints, characterizing interactions to enable a classical *degrees-of-freedom* (DOF) perspective on state variables and contraints. By this feature, disturbance propagation can be modeled effectively using the causality assignment offered by influencer roles [20].

Another important concept of abstraction is called *execution levels* [20]. The execution level concept expresses the aggregation and transformation of a set of related actions

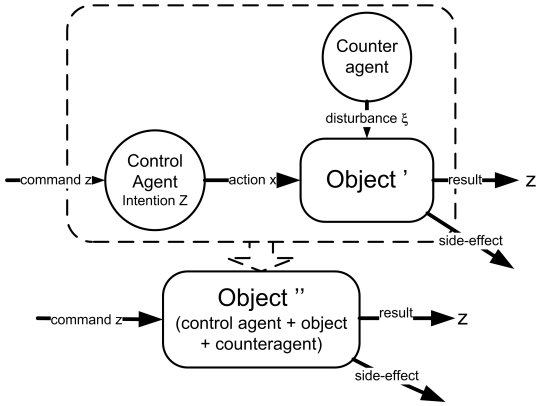

Fig. 2. Encapsulation of disturbance by a control agent. The introduction of a control agent implicitly models a virtual counter-agent.

to a single 'abstracted' action. This concept is particularly helpful to model the purpose of a control function in terms of encapsulation of counter-agents, as illustrated inf Figure 2. Execution levels are the main concept enabling the following results.

In addition to the *performative* perspective employed for execution levels, the action concept also lends itself to a *modal* perspective, which focusses on enablement of functions and control actions as interventions, which can be employed for example to derive startup plans [15].

C. Model case

To illustrate the composition of an MFM model, we provide an example modeling a basic pumping / water-circulation / heat transfer pattern, see Figure 3, which occurs in thermal power plants or central heating systems. The lower level structure represents the mass flow circulation of the lubricant (MFS2), enabling the operation (transfer of energy to the water) of the pump (tra2); the energy stored in the mass inertia is lost to a) useful energy (sin1) and b) friction (sin2). The energy transfer (pump, tra2) is actuated by the control function mco1 which aims to achieve obj1, which is in turn associated with the mass flow (water circulation). Note that objectives obj3 and obj4 refer to performance requirements for the control functions mco1 and mco2, respectively. This example is dicusssed in more detail in [19].

III. Modeling Control Purpose

While in control design, an objective is generally perceived as external requirement to the design problem, in control structure design (control configuration), the choice of control objectives in relation to the process is a central design task. To support such development with formal methodology, the relation between process and control purpose needs to be explored.

The purpose of a control function, in a general sense, is to *achieve* its control objective. To understand the role of control functions in a process context, we have to understand the meaning of these control objectives in relation to a process.

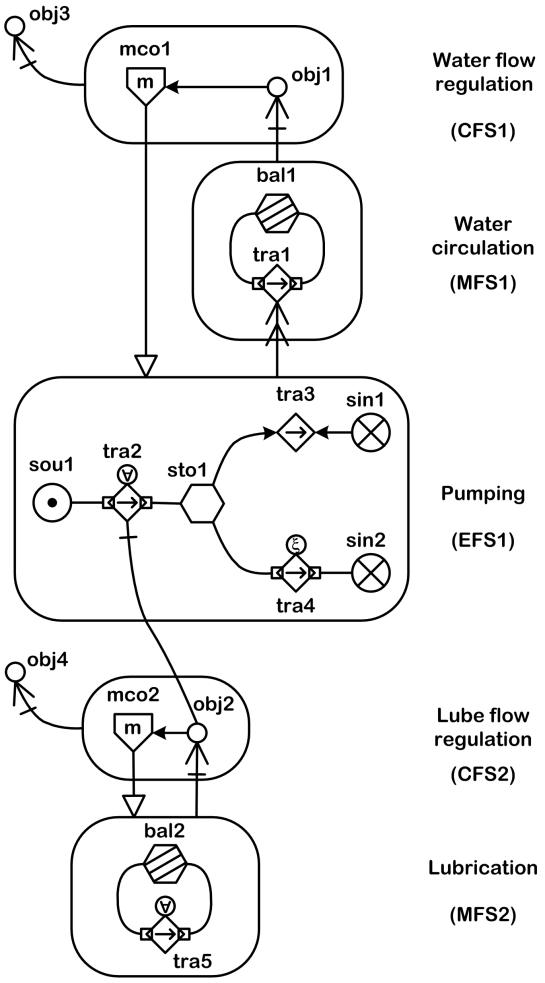

Fig. 3. Multilevel flow model of a circulation pump and water circulation with control functions [19]. On the next higher level, these function structures can be associated with a heat transfer system (e.g. [22]).

A. A Taxonomy of Control Objectives

An objective is an end stated in context of a means. MFM offers a logically reduced set of means-ends relations establishing the possible relations between functional means and objectives. Identifying the various patterns of anchoring objectives within MFM models, we can provide a taxonomy of objectives. We identify three main types of objectives:

1) *External objectives*, which have to be taken as a purpose in themselves; this category includes system service objectives, such as the room-temperature provided by a heating system, or obj1 in Figure 3;
2) *Functional objectives*, which can directly be related to a functional purpose in the model context; e.g. energy transfer to produce water circulation (Fig. 3);
3) *Situational objectives*, are indirectly related to a further purpose in the model context: the objective describes an operational condition of the system, the achievement of which enables, disables, in general satisfies or creates the condition for other functions to perform; example: lube oil flow as a condition for pump operation.

External objectives thus clearly can be viewed as control objectives. However, not all control objectives in a process follow a clear hierarchical decomposition of high-level / external objectives. On the other hand, a *functional objective* directly relates to functions to another in a means-ends relation: the *mediate* or *producer-product* relations. E.g. the energy converted in a pump *produces* a mass-transport, and the circulation of water *mediates* a heat-transfer. Such objectives do not suit as control objectives as they directly express 'physical' process couplings. Further considerations regarding the connection between functional and structural representatons are discussed in [23] – the subject is relevant in particular with regard to the management of redundancy but is beyond the scope of this paper.

Situational objectives thus remain to be investigated. Using MFM concepts, we identify:

- Objective connected to a *enable* or disable relation (e.g. the lube oil flow enables rotation),
- An objective within a control structure assuming an *actuator role* with respect to an actuate-relation; this situation corresponds to a classical control cascade where a lower-level controller is tracking the reference provided by another control function.

These types of objectives are likely control objectives. Both function and failure consequence in relation to these objectives are explicitly identified in an MFM model of a process.

B. "Folding" of a Control Function

An important but less obvious type of process-related purpose of a control function can be understood by means of the execution-level concept.

As illustrated in Figure 2, the performance of a control function is aimed at encapsulating a disturbance. It is also seen that the encapsulation results in a 'higher-level', more abstract description of the system as a new object in which the disturbance is either eliminated or its effect is propagated through the system by means of the control.

A control objectives imposes a constraint on system which 'eliminates' a degree of freedom[1] in the controlled subsystem. The successful control function realizes the objective's constraint – for example, a level-control constrains the DOF of the storage to the the value defined by the objective. A control function utilizes the influence offered by an actuator to track and eliminate the influence of a disturbance on its control objective.

As a result, the closed-loop causal structure of the system differs from the 'open-loop', uncontrolled causal structure. Using MFM as a modeling approach, this transformation can be captured formally by either representing the system in the control-encapsulated or 'folded' view or in the control-explicit view. The two views are illustrated by the example in Figure 4, which is further explained in the following example.

[1]A classical DOF concept is considered: each storage adds a state variable, each constraint reduces the DOF. Note that the DOF concept in MFM has been introduced in [20] and could use a precise definition – however, the DOF analysis concepts introduced in [3]: control-DOF vs. optimization-DOF can easily be related to the DOF in MFM concepts.

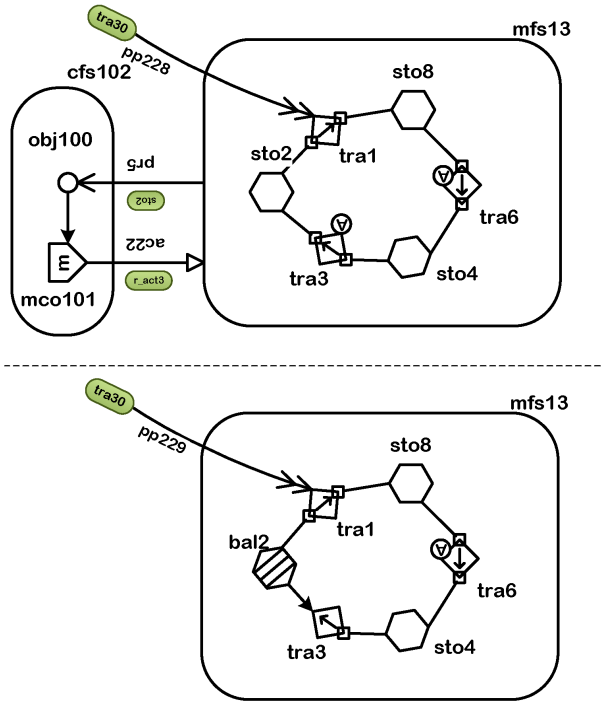

Fig. 4. Two variants of a simple model of water mass-flow circulation loop of a power plant (Full model in [20]). The upper representation shows the explicit control model and the lower shows the implicit, 'folded' function of the control.

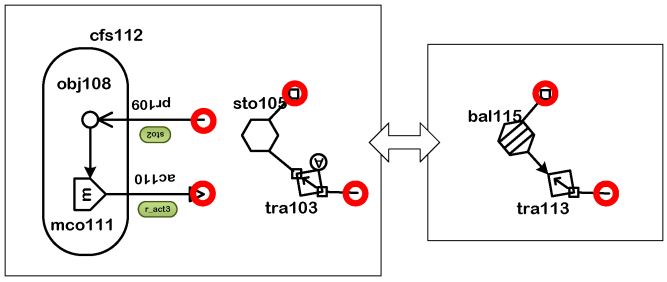

Fig. 5. Isolation of the function patterns which become altered between the control-explicit and the control-folded view of the system.

C. Example: Power Plant Water Circulation

Consider the partial MFM model provided in Figure 4. It represents a part of the heat-transfer in a thermal power plant [20]. The three storages represent the liquid phase in and before the boiler and the level-controlled tank (sto2) for which fresh water is provided as soon as some is removed, the steam phase before the turbine (sto8) and the gas-liquid mix in the turbine-condenser system between turbine inlet and feedwater pump. The water evaporation, tra1, causes removal of mass from storage 2; a level controller (obj100, mco101) actuates the feedwater pump (tra3), which thus fills up the boiler reservoir at the rate at which water is removed from sto2. The lower view of the model is control-folded: the

control function as well as the storage DOF disappears and only its effect on the causal structure of the process remains relevant.

The model-transformation between both views is identified by Figure 5: The control function and objective disappear, and the storage function get's replaced by a balance. Further, due to the reduced degree of freedom, the causal structure is altered according to the control configuration. The linking points between the remaining function-structure and the altered function-structure are identified by red circles.

D. "Failure Mode" Implication for Diagnostic Reasoning

Causal reasoning approaches for MFM models currently include root-cause and consequence analysis (for diagnosis) (e.g. [24]) and influence-path analysis [20]. These propagation approaches cannot directly be applied to reason about control functions, which is implied by the complexity of interactions of control and functions analyzed above. However, they could easily be applied for control-folded models. The 'loop' of causality which is caused by a closed control loop can thus be modeled by the resulting effective process behaviour. This means for reasoning applications, such as those discussed in [20], [24], control functions do not per se impede the applicability of the reasoning approach. As long as the studied process causality is modified according to the respective execution level, diagnosis is feasible without explicit regard for control functions.

When a control function can be identified to have failed or is de-activated, the 'external' failure mode (from a process-perspective) of the control function, would be represented by a fall-back to the un-encapsulated detailed model, just without the control function. Whether MFM can be employed to represent and reason about internal failure modes and causes of control functions is another question.

To enable this functionality, a meta-reasoning strategy will be required to manage the different representations and to allocate reasoning tasks. Further, a separate monitoring and/or reasoning function would be needed to assess whether the modelled control functions are operating as intended. With such functionality enabled, both diagnostic and planning (re-configuration) functionality would be supported.

IV. Discussion of Applications

Applications of MFM have been mentioned above, however, there are further less explored but promising applications in relation to control systems. In this section we explore useful features of MFM for the conceptual modeling of control structures. We will outline two particular application perspectives of MFM models: a) (offline) control structure design, and b) the relation to decision support systems in (online) supervisory control.

A. Control Structure Design

Due to the DOF-preserving properties of MFM models in connection with the recently introduced control roles [20], as well as for the consistent and well-motivated abstraction concepts, MFM exhibits properties that make it particularly suited for the conceptual design of control structure. Consider the method for control structure design introduced by Skogestad et al. [3]:

TOP-DOWN ANALYSIS

1) Primary Controlled Variables *(c)*
   identify primary controlled variables mainly DOF & self-optimizing variables analysis
2) Production Rate & Inventory Control
   design for (economic) optimal throughput.

MFM exhibits the properties required for the qualitative aspects of the top-down analysis. It thereby enables *problem formulation* for the second part:

BOTTOM-UP DESIGN

1) Regulatory Control Layer:
   Stabilization & Local Disturbance Rejection
2) Supervisory Control Layer:
   Control structure for primary controlled variables
3) Real-time Optimization: optimal setpoints for *(c)*.

The applicability of MFM for such design and planning tasks has been investigated in [2] in application to electric power systems.

B. Resilient Operation

A supervisory control system that would aim to enable system operation beyond the design disturbances needs to be aware of overall operation objectives and priorities and be able to relate available resources to the achievability of these objectives. Fault-tolerant control (FTC) enables an improved resilience in control. Yet, every control design must be limited to a practical scope. For FTC this scope includes a set of fault-behaviours for which the FTC is tolerant.

To ecompass a larger operation scope, a supervision system is required to contextualize the controller function. Patton [8] writes "[t]he supervision system manages the fault decision information [...]" and " must also determine whether a fault has a detrimental effect on the system's performance and stability [...]". A supervisable FTC should thus supply information about the state of system degradation, which in relation to its design specification. Existing fault-detection and identification (FDI) systems generate such information, and it can be mapped to MFM function states. The residuals generated by a FDI system supply exactly this type of information for diagnostic reasoning [11]. When this information is combined with a functional model (MFM model), the system state can be explicitly related to system operation objectives. To enable further resiliency, also counter-action planning has to be included in the operation intelligence. While still in an early stage, it has been shown that MFM can also be employed to generate counteraction plans [12].

C. Design and Operation: Two Perspectives

The applicability of MFM models in both control structure design and in support of system operation is not an accidental. MFM has been developed to create consistent

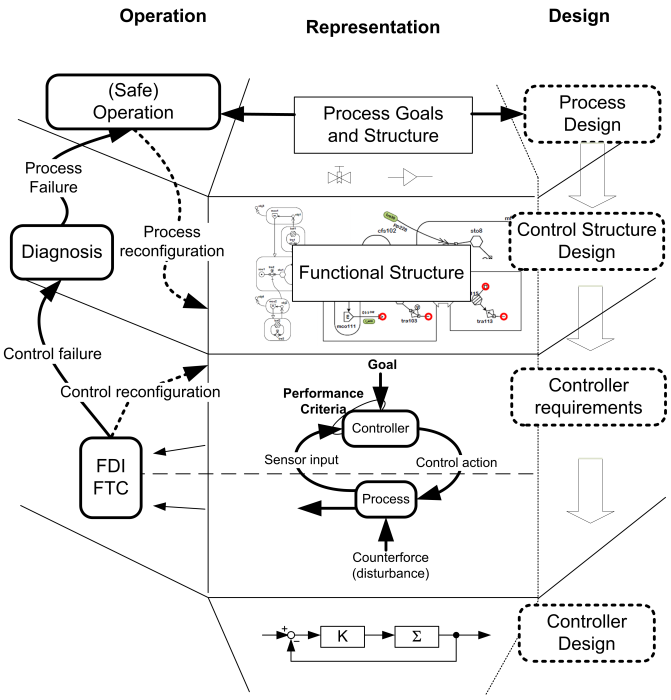

Fig. 6. Relationship of types Process/Control knowledege representation to applications in control design and operation.

representations of industrial processes where operating goals can be related to system functions. Figure 6 sketches the role of MFM representations in context of other types of knowledge representations for analysis, as well as in relation to two application perspectives: Operation and Design. Across all perspectives, several layers can be distinguished: Goals, Functions, Normative Behaviour and Realization – from ends at the top to means at the bottom. In the center, MFM models appear as a form of knowledge representation, in context of lower-level and higher-level representations.

V. Conclusion

MFM has been developed with an original motivation to make operation of nuclear power plants safer. Today, many other application domains have been discovered and the utility for MFM models beyond diagnostic reasoning is becoming apparent. The concepts developed within MFM enable access to a deeper understanding of dependencies and interactions, provide meaningful decompositions and abstraction concepts, in particular to understand and analyze the relation between control and process.

A methodological advancement has been presented, new and future applications of MFM have been outlined. The concepts of MFM offer a unique contribution to the analysis, design and operation of complex systems.

Acknowledgment

The authors would like to thank Roberto Galeazzi for good discussions and opening a new alley of collaboration.

References

[1] A. Foss, "Critique of chemical process control theory," *Automatic Control, IEEE Transactions on*, vol. 18, no. 6, pp. 642 – 652, dec 1973.

[2] K. Heussen, "Control architecture modeling for future power systems," Ph.D. dissertation, Technical University of Denmark, 2011.

[3] S. Skogestad, "Control structure design for complete chemical plants," *Computers & Chemical Engineering*, vol. 28, no. 1-2, pp. 219 – 234, 2004, escape 12. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0098135403001984

[4] T. Larsson and S. Skogestad, "Plantwide control - a review and a new design procedure," *Modeling, Identification and Control*, vol. 21, no. 4, pp. 209–40, 2000. [Online]. Available: http://www.mic-journal.no/PDF/2000/MIC-2000-4-2.pdf

[5] G. Dauphin-Tanguy, A. Rahmani, and C. Sueur, "Bond graph aided design of controlled systems," *Simulation Practice and Theory*, vol. 7, no. 5-6, pp. 493–513, Dec. 1999.

[6] S. Mattson, H. Elmqvist, and J. Broenink, "Modelica: An international effort to design the next generation modeling language," *A. Special issue on CACSD*, vol. 38, no. 3, pp. 22–25, 1997.

[7] J. Rasmussen, *Information Processing and Human Machine Interaction*. New York: North Holland, 1986.

[8] R. J. Patton, "Fault Tolerant Control: The 1997 Situation," in *IFAC Safeprocess'97*, Hull, United Kingdom, Aug. 1997, pp. 1033–1055.

[9] M. Lind, "An introduction to multilevel flow modelling," *International Journal of Nuclear Safety and Simulation*, vol. 2, no. 1, 2011.

[10] ——, "The what, why and how of functional modelling," in *Proceedings of International Symposium on Symbiotic Nuclear Power Systems for the 21'st Century (ISSNP)*, Tsuruga, Japan, July 9-11 2007, pp. 174–179.

[11] G. Gola, M. Lind, H. P.-J. Thunen, A. P.-J. Thunen, E. Wingsted, and D. Roverso, "Multilevel Flow Modeling for Nuclear Power Plant Diagnostics," in *ESREL 2011, Troyes, France*, 2011.

[12] A. Gofuku and Y. Tanaka, "Application of Derivation Technique of Possible Counter Actions to an Oil Refinery Plant," in *Proc. 4'th IJCAI Workshop on Engineering Problems for Qualitative Reasoning*, Stockholm, 1999, pp. 77–83.

[13] N. L. Rossing, M.Lind, N. Jensen, and S. B. Jørgensen, "A goal based methodology for hazop analysis," in *Proc. 4.th International Symposium on Cognitive System Engineering Approach to Power Plant Control (CSEPC2008)*, Harbin, Heilongjiang, China, September 8-10 2008.

[14] J. E. Larsson, "Diagnosis based on explicit means-end models." *Artificial Intelligence*, vol. 80(1), pp. 29–93, 1996.

[15] M. N. Larsen, "Deriving action sequences for start-up using multilevel flow models," Ph.D. dissertation, Department of Automation, Technical University of Denmark, 1993.

[16] L. E. de Souza and M. M. Veloso, "AI planning in supervisory control systems," in *Proc. IEEE International Conference on Systems, Man and Cybernetics*, Beijing, October 14-15 1996, pp. 3153–3158.

[17] A. Gofuku and Y. Tanaka, "Development of an Operator Advisory System: Finding Possible Counter Actions in Anomalous Situations," in *Proc. 5'th International Workshop on Functional Modeling of Complex Technical Systems*, Paris, France, July 1-3 1997, pp. 87–97.

[18] H. P.-J. Thunen, A. P.-J. Thunen, and M. Lind, "Using an Agent-Oriented Framework for Supervision, Diagnosis and Prognosis Applications in Advanced Automation Environments," in *ESREL, Troyes, France*, 2011.

[19] M. Lind, "Control Functions in MFM: Basic principles," *International Journal of Nuclear Safety and Simulation*, vol. 2, no. 2, 2011.

[20] K. Heussen and M. Lind, "Representing causality and reasoning about controllability of multi-level flow-systems," in *Proceedings of the 2010 IEEE Conference on Systems, Man and Cybernetics, Istanbul, Turkey*, 2010.

[21] M. Lind, "Modeling goals and functions of control and safety systems in MFM," in *Proceedings International Workshop on Functional Modeling of EngineeringSystems*, Kyoto, Japan, January 25 2005, pp. 1–7.

[22] M. Lind, H. Yshikawa, S. B. Jørgensen, M. Yang, K. Tamayama, and K. Okusa, "Multilevel flow modeling of monju nuclear power plant," in *ICI2011 (ISOFIC, CSEPC, ISSNP 2011), Daejeon, Korea*, 2011.

[23] M. Lind, "Knowledge representation for integrated plant operation and maitenance," in *7th ANS Int. Topical Meetingon Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies, NPIC&HMIT 2010*, 2010.

[24] ——, "Reasoning about Causes and Consequences in Multilevel Flow Models," in *ESREL 2011, Troyes, France*, 2011.